IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

(Attorney Docket No. 14177US02)

In the Application of:

Ed H. Frank

Serial No. 10/658,310

Filed: September 9, 2003

For: METHOD AND SYSTEM FOR PROVIDING MULTIPLE ENCRYPTION IN A MULTI-BAND MULTI-PROTOCOL HYBRID WIRED/WIRELESS NETWORK

Examiner: Carlton Johnson

Group Art Unit: 2436

Confirmation No. 2145

Electronically Filed on November 23, 2009

APPEAL BRIEF

Mail Stop Appeal Brief – Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

This is an appeal from an Office Action mailed on May 7, 2009 ("Final Office Action"), in which claims 1-42 were finally rejected. The Appellant respectfully requests that the Board of Patent Appeals and Interferences ("Board") reverse the final rejection of claims

1-42 of the present application. The Appellant notes that this Appeal Brief is timely filed within the period for reply that ends on November 23, 2009.

REAL PARTY IN INTEREST

(37 C.F.R. § 41.37(c)(1)(i))

Broadcom Corporation, a corporation organized under the laws of the state of California, and having a place of business at 5300 California Avenue, Irvine, California 92617, has acquired the entire right, title and interest in and to the invention, the application, and any and all patents to be obtained therefor, as set forth in the Assignment recorded at Reel 014222, Frame 0368 in the PTO Assignment Search room.

RELATED APPEALS AND INTERFERENCES
(37 C.F.R. § 41.37(c)(1)(ii))

The Appellant is unaware of any related appeals or interferences.

STATUS OF THE CLAIMS
(37 C.F.R. § 41.37(c)(1)(iii))

The present application includes pending claims 1-42, all of which have been rejected. Claims 1, 6-9, 12-15, 20-23, 26-29, 34-37 and 40-42 are rejected under 35 U.S.C. § 103(a) as being unpatentable over USPP 20030140131 ("Chandrashekhar") in view of USP 6,751,729 ("Giniger"), and further in view of USP 7,174,564 ("Weatherspoon"). Claims 2-5, 10, 11, 16-19, 24, 25, 30-33, 38 and 39 are rejected under 35 U.S.C. § 103(a) as being unpatentable over Chandrashekhar, Giniger and

Weatherspoon, and further in view of USP 6,088,451 ("He"). The Appellant identifies claims 1-42 as the claims that are being appealed. The text of the pending claims is provided in the Claims Appendix.

STATUS OF AMENDMENTS
(37 C.F.R. § 41.37(c)(1)(iv))

The Appellant has not amended any claims subsequent to the final rejection of claims 1-42 mailed on May 7, 2009.

SUMMARY OF CLAIMED SUBJECT MATTER
(37 C.F.R. § 41.37(c)(1)(v))

The Appellant has inserted Figs. 3, 4, 5 and 6 of the present application below, to illustrate one aspect of the invention.

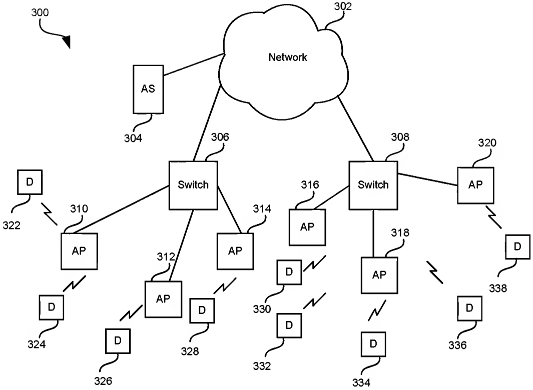
300
302
Network
AS
304
306
Switch
308
Switch
320
AP
316
AP
310
AP
314
AP
312
AP
318
AP
D
322
D
324
D
326
D
328
D
330
D
332
D
334
D
336
D
338

FIG. 3

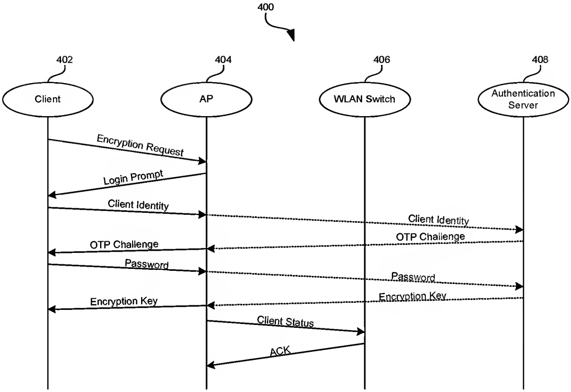
400
402
404
406
408
Client
AP
WLAN Switch
Authentication Server
Encryption Request
Login Prompt
Client Identity
Client Identity
OTP Challenge
OTP Challenge
Password
Password
Encryption Key
Encryption Key
Client Status
ACK

FIG. 4

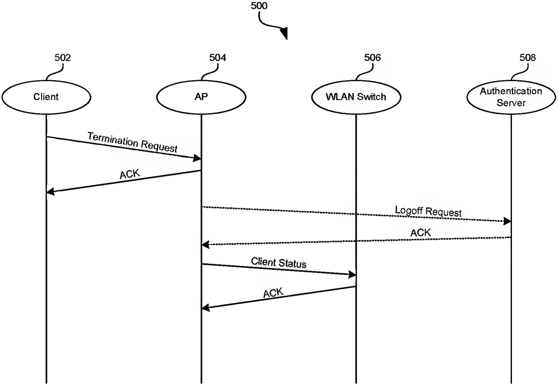
500
502
504
506
508
Client
AP
WLAN Switch
Authentication Server
Termination Request
ACK
Logoff Request
ACK
Client Status
ACK

FIG. 5

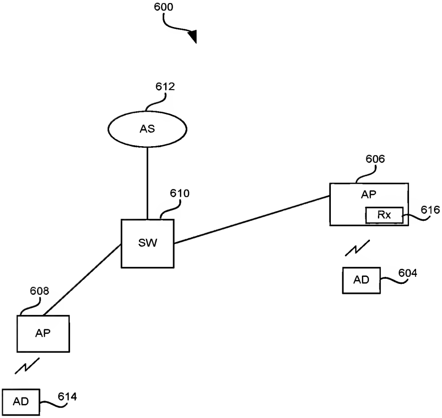

FIG. 6

The invention of claim 1 is illustratively described in, for example, the "Brief Summary of the Invention" section, as well as in the description of Figs. 1a-5. For example, aspects of the invention provide a method and system for multiple encryption (i.e., multiple encryption requests/keys and authentications in Fig. 4) in a multi-band multi-protocol hybrid wired/wireless network (e.g., hybrid wired/wireless LAN 200 and 300 of Figs. 2 and 3, respectively). *See* present application at page 8, lines 2-3. A method for multiple encryption (i.e., multiple encryption keys and authentications in Fig.

4) in a multi-band multi-protocol hybrid wired/wireless network (e.g., hybrid wired/wireless LAN 200 and 300 of Figs. 2 and 3, respectively) may include the step of receiving on a first PHY channel of an access point (e.g., AP 404 in Fig. 4 or AP 504 in Fig. 5), a request (e.g., encryption request from client 402 to AP 404 in Fig. 4) for initiation of a communication session from an originating access device (e.g., client 402 in Fig. 4 or client 502 in Fig. 5). *See id.* at page 8, lines 3-6. The received request may be acknowledged (e.g., sending an ACK from AP 504 to client 502 in Fig. 5) on the first PHY channel. *See id.* at page 8, lines 6-7. The originating access device (e.g., client 402 in Fig. 4 or client 502 in Fig. 5) may be authenticated (e.g., authenticating server 408 authenticates client identity such as a WEP key, a MAC address, and/or an IP address in Fig. 4) using a second PHY channel. *See id.* at page 8, lines 7-8. A communication session may be hosted over the first PHY channel, the second PHY channel or a third PHY channel (where claim 1 recites a communication session may be hosted over a third PHY only). *See id.* at page 8, lines 8-9.

Claims 2-14 are dependent directly or indirectly upon independent claim 1.

The invention of claim 15 is illustratively described in, for example, the "Brief Summary of the Invention" section, as well as in the description of Figs. 1a-5. For example, another embodiment of the invention may provide a machine-readable storage, having stored thereon, a computer program having at least one code section for providing multiple encryption (i.e., multiple encryption keys and authentications in Fig. 4) in a multi-band multi-protocol hybrid wired/wireless environment (e.g., hybrid wired/wireless LAN 200 and 300 of Figs. 2 and 3, respectively). *See id.* at page 8, line 26 to page 9, line 2. The at least one code section may be executable by a machine and thereby cause the machine to perform the steps as described above. *See id.* at page 9, lines 2-3. More specifically, the steps may include: the step of receiving on a first PHY channel of an access point (e.g., AP 404 in Fig. 4 or AP 504 in Fig. 5), a request (e.g., encryption request from client 402 to AP 404 in Fig. 4) for initiation of a communication session from an originating access device (e.g., client 402 in Fig. 4 or client 502 in Fig. 5). *See id.* at page 8, lines 3-6. The received request may be acknowledged (e.g., sending an ACK from AP 504 to client 502 in Fig. 5) on the first PHY channel. *See id.* at page 8, lines 6-7. The originating access device (e.g., client 402 in Fig. 4 or client 502 in Fig. 5) may be authenticated (e.g., authenticating server 408 authenticates client identity such as a WEP key, a MAC address, and/or an IP address in Fig. 4) using a second PHY channel. *See id.* at page 8, lines 7-8. A communication session may be hosted over the first PHY channel, the second PHY channel or a third PHY channel (where claim 14 recites a communication session may be hosted over a third PHY only). *See id.* at page 8, lines 8-9.

Claims 16-28 are dependent directly or indirectly upon independent claim 14.

The invention of claim 29 is illustratively described in, for example, the "Brief Summary of the Invention" section, as well as in the description of Figs. 1a-5. For example, another embodiment of the invention may provide a system for multiple encryption (i.e., multiple encryption keys and authentications in Fig. 4) in a multi-band multi-protocol hybrid wired/wireless network (e.g., hybrid wired/wireless LAN 200 and 300 of Figs. 2 and 3, respectively). The system may include an access point (e.g., AP 404 in Fig. 4 or AP 504 in Fig. 5) having at least one receiver which may be adapted to receive a request (e.g., encryption request from client 402 to AP 404 in Fig. 4) for initiating a communication session from an originating access device (e.g., client 402 in Fig. 4 or client 502 in Fig. 5). The initiation request (e.g., encryption request from client 402 to AP 404 in Fig. 4) may be received on a first PHY channel of the access point (e.g., AP 404 in Fig. 4 or AP 504 in Fig. 5). The receiver may be adapted to acknowledge the received request (e.g., encryption request from client 402 to AP 404 in Fig. 4) on the first PHY channel. At least one authenticator (e.g., authenticating server 408 authenticates client identity such as a WEP key, a MAC address, and/or an IP address in Fig. 4) may be adapted to authenticate the originating access device (e.g., client 402 in Fig. 4 or client 502 in Fig. 5) using a second PHY channel. The first PHY channel, second PHY channel and/or a third PHY channel may be adapted to facilitate hosting of the communication session (where claim 29 recites a communication session may be hosted over a third PHY only). *See id.* at page 9, lines 11-13.

Claims 30-42 are dependent directly or indirectly upon independent claim 29.

GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL
(37 C.F.R. § 41.37(c)(1)(vi))

Claims 1, 6-9, 12-15, 20-23, 26-29, 34-37 and 40-42 are rejected under 35 U.S.C. § 103(a) as being unpatentable over USPP 20030140131 ("Chandrashekhar") in view of USP 6,751,729 ("Giniger"), and further in view of USP 7,174,564 ("Weatherspoon"). Claims 2-5, 10, 11, 16-19, 24, 25, 30-33, 38 and 39 are rejected under 35 U.S.C. § 103(a) as being unpatentable over Chandrashekhar, Giniger and Weatherspoon, and further in view of USP 6,088,451 ("He").

ARGUMENT

(37 C.F.R. § 41.37(c)(1)(vii))

REJECTION UNDER 35 U.S.C. § 103

In order for a *prima facie* case of obviousness to be established, the Manual of Patent Examining Procedure, Rev. 6, Sep. 2007 ("MPEP") states the following:

> The key to **supporting** any rejection under 35 U.S.C. 103 is the **clear articulation** of the reason(s) why the claimed invention would have been obvious. The Supreme Court in KSR International Co. v. Teleflex Inc., 82 USPQ2d 1385, 1396 (2007) noted that **the analysis supporting a rejection under 35 U.S.C. 103 should be made explicit**. The Federal Circuit has stated that "rejections on obviousness cannot be sustained with mere conclusory statements; instead, there must be some articulated reasoning with some rational underpinning to support the legal conclusion of obviousness."

See the MPEP at § 2142, citing *In re Kahn*, 441 F.3d 977, 988, 78 USPQ2d 1329, 1336 (Fed. Cir. 2006), and *KSR International Co. v. Teleflex Inc.*, 82 USPQ2d at 1396 (quoting Federal Circuit statement with approval). Further, MPEP § 2143.01 states that "the mere fact that references can be combined or modified does not render the resultant combination obvious unless the results would have been predictable to one of ordinary skill in the art" (citing *KSR International Co. v. Teleflex Inc.*, 82 USPQ2d 1385, 1396 (2007)). Additionally, if a *prima facie* case of obviousness is not established, the Appellant is under no obligation to submit evidence of nonobviousness:

> The examiner bears the initial burden of factually supporting any *prima facie* conclusion of obviousness. If the examiner does not produce a *prima facie* case, the Appellant is under no obligation to submit evidence of nonobviousness.

See MPEP at § 2142.

I. The Proposed Combination of Chandrashekhar, Giniger and Weatherspoon Does Not make Claims 1, 15 and 29 Unpatentable

A. Independent Claims 1, 15 and 29

With regard to the rejection of claims 1, 15, and 29 under 35 U.S.C. 103(a), the Appellant submits that the combination of Chandrashekhar, Giniger and Weatherspoon does not disclose at least the limitation of "**authenticating** said communication session by authenticating said **originating access device using a second PHY channel; and hosting said communication session over a third PHY channel, said third PHY channel established between said access point and said originating access device**," as recited in independent claims 1, 15, and 29.

In order to help understanding, the Appellant has inserted Weatherspoon's Fig. 2 for reference:

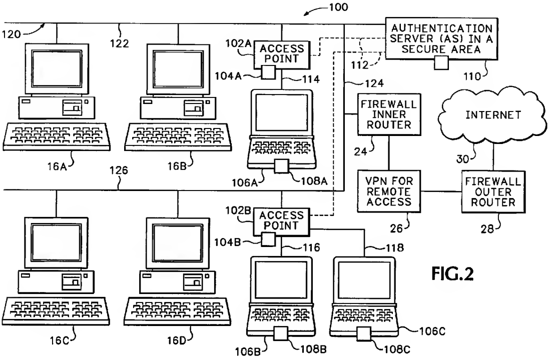

FIG.2

The Examiner states the following in the Final Office Action:

"With Regards to Claims 1, 15, 29, Chandrashekhar discloses a method, machinereadable storage having stored upon a computer program having at least one code section, system for multiple encryption in a multi-band multi-protocol hybrid wired/wireless network, the method comprising: **receiving on a first PHY channel of an access point**, a request for initiation of a communication session from an originating access device; authenticating said communication session by **authenticating said access using a second PHY channel**; and **hosting said communication session over a third PHY channel** , said third PHY channel established between said access point and said originating access device. (see Chandrashekhar paragraph [0054], lines 3-5; paragraph [0054], lines 10-12: hybrid communications network; paragraph [0040], lines 4-6; paragraph [0108], lines 1-5: wireless/wired communications; paragraph [0056], lines 1-3: request for communications service; paragraph [0048], lines 1-7: software, implementation means); Figure 3; paragraph [0112], lines 1-5; paragraph [0112], lines 27-28: access point communications device(s))"

See the Final Office Action at page 5 (emphasis added). The Examiner relies for support on Chandrashekhar's Fig. 3, and equates Chandrashekhar's Virtual Private Network (VPN) to Appellant's hybrid wired/wireless network. Even though Chandrashekhar discloses various access devices (the alleged "originating access device"), Chandrashekhar (in the cited paragraphs [0040], [0048], [0054], [0056], [0108] and [0112], or in the entire reference), does not disclose an access point, let alone disclose a first PHY channel, a second PHY channel and a third PHY channel in an access point.

The Examiner argued the following in the Advisory Office Action:

> "Chandrashekhar prior art discloses a ...communications link between two network nodes to perform an authentication procedure... discloses communications completed over **a wireless communications network using access points**. (see Chandrashekhar paragraph [0112], lines 1-5; paragraph [0112], lines 27-28)."

The Examiner relies for support on the following citation of Chandrashekhar:

> "The above-described D-VPN technology combines IP bandwidth management, IP VPN, and Directory Enabled Networking technologies in a novel and unique way to provide a platform that extends current ISP network capabilities to include: (1) A single user interface for the management of IP VPN services.... (10) Automated activation and deactivation of the above capabilities based on temporal and repetitive parameters (11) Providing the above capabilities over **a wireless access network**;.."

See Chandrashekhar at paragraph [0112], lines 1-5; lines 27-28 (emphasis added). As seen from the above citation, Chandrashekhar merely discloses a **wireless access network** (the alleged "hybrid wired/wireless network"), but it does not disclose an access point, as alleged by the Examiner. Even assuming that an access point may be used somewhere in Chandrashekhar wireless network, the Examiner's argument is still deficient, because **Chandrashekhar still does not disclose using the respective first, second and third PHY channels of an access point to perform the multiple encryption process on an originating access device**, as recited in Appellant's claim 1.

The Examiner concedes the following regarding the Chandrashekhar reference:

> "Chandrashekhar does not specifically disclose whereby **authenticating said originating access device**. However, Giniger discloses wherein authenticating said originating access device. (see Giniger col. 3, lines 21-25: VPN (tunnel) communications; col. 4, lines 59-67; col. 5, lines 6-10; col. 15, lines 27-33: authentication, network device)"

See the Final Office Action at page 5 (emphasis added). The Examiner looks for support to Ginger, and equates Ginger's authenticating node device by the server (*see* Ginger at col. 4, lines 59-67) to Appellant's "authenticating said originating access device". Ginger, however, does not disclose a hybrid wired/wireless network. For example, Giniger merely discloses multiple computers coupled to a router data base for centralized encryption in a wired network. **Giniger does not disclose a hybrid network**, let alone discloses "authenticating said originating access device" (i.e., within the hybrid network), as recited in Appellant's claim 1. In addition, **Ginger also does not** overcome Chandrashekhar's deficiencies, namely, it does not **disclose "an access point"** with respective first, second and third PHY channels. Therefore, Ginger does not overcome any of Chandrashekhar's above deficiencies.

Based on the above rationale, the Examiner is required to cite for factual support from Weatherspoon to overcome the deficiencies of Chandrashekhar and Ginger. Namely, the deficiencies of Chandrashekhar and Ginger include: (1) neither disclose an access point with the respective first, second and third PHY channels; (2) neither disclose that the respective first, second and third PHY channels perform the functions of "receiving on a first PHY channel of an access point, a request for initiation of a communication session from an originating access device; authenticating said communication session by authenticating said originating access device using a second PHY channel"; and (3) neither disclose "hosting said communication session over a third PHY channel, said third PHY channel established between said access point and said originating access device," as recited in Appellant's claim 1.

The Appellant now turns to the arguments regarding the Weatherspoon reference. Regarding Weatherspoon, the Examiner states the following in the Final Office Action:

> "In addition, Weatherspoon discloses wherein a method, machine-readable storage having stored upon a computer program having at least one code section, system for multiple encryption in a multi-band multi-protocol hybrid wired/wireless network, the method comprising: receiving on a first PHY channel of an access point, a request for initiation of a communication session from an originating access device (see Weatherspoon col. 4, lines 23-29: plurality of APs and corresponding devices; col. 4, lines 32-37: establishes a communications channel); authenticating said communication session by **authenticating said access using a second PHY channel** (see Weatherspoon col. 5, lines 12-19: if the wireless device is valid **the AP establishes a control channel with the authentication server**;..."

See the Final Office Action at page 6. The Examiner relies for support on Weatherspoon's Fig. 2, and equates Weatherspoon's **wireless device** (one of wireless laptops 106A to 106C), AP 102A and access to the devices on the wired LAN 120 by the wireless device through the AP 102 to Appellant's "**originating access device**", "access point" and "communication session" respectively. The Examiner equates Weatherspoon's air channel 114 (*see* step 302 in Fig. 3A) between the wireless device 106A (the alleged "originating access device") and the AP 102A (the alleged "AP") to Appellant's "first PHY channel of an access point established with an originating access device". The Examiner also equates Weatherspoon's **control channel 112 between the AP** 102A (the alleged "AP") **and the authentication server** 110 to "authenticating said communication session by **authenticating said originating access device using a second PHY channel,**" as recited in Appellant's claim 1.".

The Appellant points out that even though Weatherspoon's control channel 112 (the alleged "second PHY channel" of AP 102A) is used to transmit the first authentication message of the AP 102A and the second authentication message of the operator's logon name and password (*see* Weatherspoon at col. 4, lines 13-19) to be verified by the authentication server 110, Weatherspoon nevertheless, **discloses that the actual authentication of the wireless laptop device 106A** (i.e., the alleged "originating access device") **takes place over air channel 114** (the alleged "first PHY channel" of AP), and not over the control channel 112 (the alleged "second PHY channel" of AP). The Examiner is referred to the following citation of Weatherspoon:

> "The AP encrypts (step 306) and transmits (step 308) the first authentication message to the wireless device 106A. The wireless device 106A receives and decrypts (step 310) the first authentication message and determines whether the AP is a valid access point to the wired LAN 120 (step 312). Authenticating the AP by analyzing the first authentication message ensures that the AP is authorized to be connected to the wired LAN 120 and that it is not a rogue AP set up to facilitate or gain unauthorized access to the wired LAN 120... If the AP 102A is valid, the second authentication device 108A generates (step 316) a second authentication message that, at a minimum, includes a device key identifying the second authentication device 108A as well as the operator ' s logon name and password. The device key may be known or unknown to the operator. **Validation of the wireless device 106A may involve a challenge response in which the AP 102A requests a certain type of validation from the wireless device 106A, e.g., a digitally signed message. The second authentication device 108A encrypts (step 318) and transmits (step 320) the second authentication message to the AP 102A** over the air channel 114. The AP 102A receives the second authentication message and decrypts the portion of the message that includes the device key. At step 322, the AP 102A analyzes the decrypted portion of the second authentication message, i.e., the device key, to determine whether the wireless device 106A is valid."

See Weatherspoon at col. 4, line 47 – col. 5, line 8 (emphasis added). Weatherspoon in the citation discloses that the validation (i.e., the alleged "authentication") of the wireless device 106A (i.e., the alleged "originating access device") is over channel 114 (the alleged "first PHY channel" of AP). In this regard, Weatherspoon does not disclose or suggest **"authenticating said originating access device using a second PHY channel,"** as recited in Appellant's claim 1. Weatherspoon therefore, at least does not overcome the above listed second deficiency of Chandrashekhar and Ginger.

Furthermore, the Examiner states the following in the Final Office Action:

> "Weatherspoon discloses ...transmits encrypted authentication messages that includes operator's logon name and password); and **hosting said communication session over a third PHY channel, said third PHY channel established between said access point and said originating access device**. (see Weatherspoon col. 5, lines 29-37: **authentication server will enable access to the wired LAN by establishing a data channel between the AP and any other device on the wired LAN)** It would have been obvious to one of ordinary skill in the art to modify Chandrashekhar to enable a first, second, and third communication channel for authentication and data transfers as taught by Weatherspoon."

See the Final Office Action at pages 6-7. The Examiner seems to equate Weatherspoon's authenticating server 110 **enabling access** to **any device on the wired LAN 120** (by the wireless device, i.e., the alleged "originating access device") via the AP 102A, to "hosting said communication session over a third PHY channel," as recited in Appellant's claim 1. In other words, the Examiner equates the "establishing data channel", which connects the AP 102A to the wired LAN 120, to Appellant's "third PHY channel" of the AP.

The Examiner's above argument is still deficient, because Weatherspoon does not disclose that the any device (i.e., computers 16A-16D's) on the wired LAN 120 are among the alleged "originating access device". For example, initially, Weatherspoon discloses that the alleged establishing or initiation of the communication session (i.e., enabling access to the any wired device 16A on the wired LAN 120 by the wireless device 108A via the AP 102A), is between the wireless device 106A (the alleged "originating access device") and the AP 102A (the alleged "AP") **over the air channel 114** (the alleged "first PHY channel of AP"). However, the wired device 16A on the wired LAN 120, is not part of the alleged establishing over the air channel 114 (the alleged "first PHY channel of AP").

On the contrary, Weatherspoon discloses that the AP 102A is for supporting and establishing communication with the wireless devices only. The Examiner is referred to the following citation of Weatherspoon:

> "A single AP can support a single wireless device e.g., **AP 102A supports wireless device 106A-or a small group of wireless devices** e.g., AP 102B supports wireless devices 106B-C."

See Weatherspoon at col. 3, lines 64-67 (emphasis added). Weatherspoon clearly discloses an example, that a single AP supports (i.e., over channel 114, the alleged "first PHY channel" of AP) a single or a small group of wireless devices 106A (i.e., the alleged "originating access device"). Weatherspoon does not disclose or suggest that the any device 16A, in the wired LAN 120, is established or supported by the AP 102A (i.e., **over the same channel 114**, the alleged "first PHY channel" of AP).

To further contrast the Examiner's argument, Weatherspoon instead discloses that the any device 16A, in the wired LAN 120, are **directly connected to the authentication server** 110. The Examiner is referred to Weatherspoon's Fig. 2 and the related description:

> "**An authentication server 110 is <u>connected to the wired LAN 120</u>**. The authentication server 110 works in conjunction with the APs 102A B and the wireless devices 106A-C and their respective authentication devices 104A-B and 108A-C to allow access only to those authorized by the network's administrators."

See Weatherspoon at col. 4, lines 17-22 (emphasis added). Weatherspoon discloses that **the wired LAN 120 is directly connected to** (i.e., without having to go through the AP 102A) the authentication server 110. In other words, **the any devices on the wired LAN 120, <u>are both directly connected to and authenticated</u> by the authentication server 110 over the wired LAN 120. Therefore, the any devices on the wired LAN 120, neither needs to be originated or authenticated over any channel of the AP 102A, namely, the respective air channel 114** (the alleged "first PHY channel" of AP) **or the control channel 112** (the alleged "second PHY channel" of AP). Therefore, the Examiner is incorrect to equate Weatherspoon's any device (i.e., computers 16A-16D's) on the wired LAN 120, to Appellant's "originating access device".

Based on the argument that Weatherspoon's **any device** (i.e., computers 16A-16D's) **on the wired LAN 120 is not the alleged "originating access device**, accordingly, the Examiner is also incorrect to equate the enabled access of the AP 102A to the wired LAN 120 (to access to the any device, i.e., computers 16A-16D's), to Appellant's "third PHY channel" of AP.

In this regard, the Appellant maintains that Weatherspoon **does not** disclose or suggest "said **third PHY channel established between said access point and said originating access device**," as recited in Appellant's claim 1.

In response, the Examiner states the following in the Advisory Office Action:

> "For claim 1, **there is no limitation that restricts the second PHY channel between the access point and the originating access**

> **device**. Claim 1 limitation states: "authenticating said communication session by authenticating said access using a second PHY channel". **The result of this communication channel is to authenticate access for communications over the third PHY channel.** The control channel or second PHY channel is used to authenticate the originating access device. Figure 4 of the application discloses that the client transmits a client identity such as a password to an authentication server for authentication. Paragraph [0025] of the specification discloses that authentication information is transferred to an authentication server using a second PHY channel. The Weatherspoon prior art disclosing the usage of an authentication server appears to be equivalent to application's usage of an authentication server..."

See the Advisory Office Action at page 2 (emphasis added). The Examiner seems to argue that the result of the authentication in the control channel 112 (the alleged "second PHY channel" of AP), includes also authenticating the any devices on the wired LAN 120. The Appellant respectfully disagrees, and refers the Examiner to Appellant's above argument, namely, Weatherspoon discloses that **the any devices on the wired LAN 120, <u>are both directly connected to and authenticated</u> by the authentication server 110 over the wired LAN 120. Therefore, the any devices on the wired LAN 120, neither needs to be originated or authenticated over any channel of the AP 102A, namely, the respective air channel 114** (the alleged "first PHY channel" of AP) **or the control channel 112** (the alleged "second PHY channel" of AP). In this regard, the Examiner's above argument that "the result of this communication channel is to authenticate access for communications over the third PHY channel," is now moot.

Likewise, the Examiner's above allegation, that "Appellant's claim 1 has no limitation that restricts the second PHY channel between the access point and the originating access device," is irrelevant and also moot. The rationale is: **Weatherspoon's any devices on the wired LAN 120 neither needs to be originated or authenticated over any channel of the AP 102A, namely, the respective air channel 114** (the alleged "first PHY channel" of AP) **or the control channel 112** (the alleged "second PHY channel" of AP),

Based on the foregoing argument, the Appellant maintains that Weatherspoon does not disclose or suggest "said third PHY channel **established between said access point and said originating access device**," as recited in Appellant's claim 1, Weatherspoon, therefore, also does not overcome the above listed third deficiency of Chandrashekhar and Ginger.

Furthermore, the Examiner argued the following in the Advisory Office Action:

> "The **authentication process enables access to any device on the wired LAN including the originating access device**. This particular access to any wired device includes establishing a data channel between the AP **and any device including the originating access device**. (Weatherspoon col. 5, lines 29-34: access between AP and any device including originating access device.)"

See the Advisory Office Action at page 2 (emphasis added). The Examiner is again referred to Appellant's above argument, namely, Weatherspoon discloses that **the any devices on the wired LAN 120, <u>are both directly connected to and authenticated</u> by the authentication server 110 over the wired LAN 120. Therefore, the any devices on the wired LAN 120, neither needs to be originated**

or authenticated over any channel of the AP 102A, namely, the respective air channel 114 (the alleged "first PHY channel" of AP) **or the control channel 112** (the alleged "second PHY channel" of AP).

Therefore, the Examiner's above allegation that the "**authentication** process **enables access to any device on the wired LAN** 122, including the originating access device. **This particular access to any wired device includes establishing a data channel between the AP and any device including the originating access device**", is contrary to Weatherspoon's disclosure, and also moot.

Accordingly, Weatherspoon's any device on the wired LAN (the alleged originating access device), is neither the alleged "originating access device", nor one being authenticated by the alleged second PHY channel of the AP 102A.

The Appellant maintains that Weatherspoon at least does not overcome the above listed second and third deficiencies of Chandrashekhar and Ginger, namely Weatherspoon does not disclose at least either "**authenticating said originating access device using a second PHY channel**," or "hosting said communication session over a third PHY channel, and **said third PHY channel established between said access point and said originating access device**" as recited in Appellant's claim 1. Therefore, the combination of Chandrashekhar, Giniger and Weatherspoon does not establish a prima facie case of obviousness to reject Appellant's claim 1. Appellant's claim 1 is submitted to be allowable. Claims 15 and 29 are submitted to be allowable based on the same rationale of claim 1.

Furthermore, the Appellant reserves the right to argue additional reasons beyond those set forth herein to support the allowability of the independent claims 1, 15 and 29 should such a need arise.

B. Dependent Claims 6-9, 12-14, 20-23, 26-28, 34-37 and 40-42

Based on at least the foregoing, the Appellant believes the rejection of independent claims 1, 15 and 29 under 35 U.S.C. § 103(a) as being unpatentable by the combination of Chandrashekhar, Giniger and Weatherspoon has been overcome and requests that the rejection be withdrawn. Claims 6-9, 12-14, 20-23, 26-28, 34-37 and 40-42 depend from independent claims 1, 15, and 29, respectively, and are, submitted to be allowable at least for the reasons stated above with regard to allowability of claim 1.

II. The Proposed Combination of Chandrashekhar, Giniger, Weatherspoon and He Does Not Render Claims 2-5, 10, 11, 16-19, 24, 25, 30-33, 38 and 39 Unpatentable

The Appellant now turns to the rejection of claims 2-5, 10, 11, 16-19, 24, 25, 30-33, 38 and 39 as being unpatentable under 35 U.S.C. §103(a) over Chandrashekhar and Giniger in view of He.

Based on at least the foregoing, the Appellant believes the rejection of independent claims 1, 15 and 29 under 35 U.S.C. § 103a as being unpatentable over Chandrashekhar and Giniger in view of Weatherspoon has been overcome. He does not overcome the deficiencies of Chandrashekhar, Giniger and Weatherspoon. Since claims 2-5, 10, 11, 16-19, 24, 25, 30-33, 38 and 39 are dependant directly or indirectly from independent claims 1, 15, and 29, respectively, the Appellant respectfully submits that the rejection of the dependent claims consequently be withdrawn and the claims 2-5, 10, 11, 16-19, 24, 25, 30-33, 38 and 39 be allowed.

A. Rejection of Dependent Claims 9 and 23

The Examiner states the following in page 4 of the Final Office Action:

> "With Regards to Claims 9, 23, Chandrashekhar discloses ...**determining** a type of traffic generated **by said originating access device** on said first PHY channel. (see Chandrashekhar paragraph [0028], lines 13-15: type of traffic, VPN; paragraph [0054], lines 7-12: between communications endpoints"

The Examiner seems to equate Chandrashekhar's VPN administrator manages various VPN services to Appellant's "**determining** a type of traffic..." Chandrashekhar however, discloses that it is the VPN administrator, not the user (the alleged "originating access device), which performs the function of "**determining** a type of traffic..." In addition, the Examiner is referred to Appellant's above argument regarding claim 1, that Chandrashekhar does not disclose the use of AP, let alone disclosing a first PHY channel on the AP. In this regard, Chandrashekhar does not disclose or suggest "**determining** a type of traffic generated **by said originating access device** on said first PHY channel," as recited in Appellant's claim 9. Giniger, Weatherspoon and He do not overcome Chandrashekhar's above deficiencies. Claim 9 is submitted to be allowable. Claim 23 is similar to claim 9 in many respects, and is also submitted to be allowable.

B. Rejection of Dependent Claims 10 and 24

The Examiner states the following in page 4 of the Final Office Action:

> "... He discloses wherein comprising generating at least one encryption/decryption key. (*see* He col. 18, lines 2-5; col. 19, lines 8-11; col. 20, lines 57-61: generation encryption/decryption key)"

The Examiner relies on He (*see* He col. 18, lines 2-5; col. 19, lines 8-11; col. 20, lines 57-61) to disclose deficiency of Chandrashekhar, Giniger and Weatherspoon, namely, "generating at least one encryption/decryption key dependent on the determined traffic type," as recited in Appellant's claim 10. Specifically He discloses generating a temporary secret key to secure communication **between the user and the network access server**. However, He still does not disclose that the generated encryption/decryption key between the user and network access server is "dependent on the determined traffic type," as recited in Appellant's claim 10. Accordingly, the Appellant maintains that and He does not overcome the deficiency of Chandrashekhar, Giniger and Weatherspoon. Claim 10 is submitted to be allowable. Claim 24 is similar to claim 10 in many respects, and is also submitted to be allowable.

C. Rejection of Dependent Claims 11, 13-14, 25, 27-28, 30-32, 38-39 and 41-42

Claims 11, 13-14, 25, 27-28, 30-32, 38-39 and 41-42 are submitted to be allowable based on their dependencies on claims 10, 24 and 29, respectively.

CONCLUSION

For at least the foregoing reasons, the Appellant submits that claims 1-42 are not rendered obvious over the combination of Chandrashekhar, Giniger, Weatherspoon and He. Reversal of the Examiner's rejection and issuance of a patent on the application are therefore requested.

The Commissioner is hereby authorized to charge $540 (to cover the Brief on Appeal Fee) and any additional fees or credit any overpayment to the deposit account of McAndrews, Held & Malloy, Ltd., Account No. 13-0017.

Respectfully submitted,

Date: November 23, 2009

/ Frankie W. Wong /

Frankie W. Wong
Registration No. 61,832
Patent Agent for Appellant

MCANDREWS, HELD & MALLOY, LTD.
500 WEST MADISON STREET, 34TH FLOOR
CHICAGO, ILLINOIS 60661
(312) 775-8093 (FWW)
Facsimile: (312) 775 – 8100

CLAIMS APPENDIX
(37 C.F.R. § 41.37(c)(1)(viii))

1. A method for multiple encryption in a multi-band multi-protocol hybrid wired/wireless network, the method comprising:

receiving on a first PHY channel of an access point, a request for initiation of a communication session from an originating access device;

authenticating said communication session by authenticating said originating access device using a second PHY channel; and

hosting said communication session over a third PHY channel, said third PHY channel established between said access point and said originating access device.

2. The method according to claim 1, comprising generating at least one encryption/decryption key for use during said communication session.

3. The method according to claim 2, wherein said authenticating comprises requesting authentication information from an authentication server.

4. The method according to claim 3, wherein said authenticating comprises delivering at least a portion of said authentication information received from said authentication server to said originating access device via said second PHY channel.

5. The method according to claim 4, comprising delivering said at least one encryption/decryption key to said originating access device via one of said first PHY channel or said second PHY channel.

6. The method according to claim 1, comprising receiving an identification of said originating access device by said access point.

7. The method according to claim 6, wherein said identity of said originating access device is one or more of a WEP key, a MAC address, and/or an IP address.

8. The method according to claim 1, comprising acknowledging said received request on said first PHY channel.

9. The method according to claim 1, comprising determining a type of traffic generated by said originating access device on said first PHY channel.

10. The method according to claim 9, comprising generating at least one encryption/decryption key dependent on said determined traffic type.

11. The method according to claim 10, comprising distributing said generated at least one encryption/decryption key via one or both of said second PHY channel and/or said third PHY channel.

12. The method according to claim 1, comprising establishing at least one virtual channel between said originating access device and a terminating access device.

13. The method according to claim 12, comprises tunneling information between said originating access device and said terminating access device.

14. The method according to claim 12, comprising establishing at least a portion of said at least one virtual channel over at least a portion of one of said first PHY channel, said second PHY channel or said third PHY channel.

15. A machine-readable storage, having stored thereon, a computer program having at least one code section for providing multiple encryption in a multi-band multi-protocol hybrid wired/wireless network, the at least one code section executable by a machine for causing the machine to perform the steps comprising:

receiving on a first PHY channel of an access point, a request for initiation of a communication session from an originating access device;

authenticating said communication session by authenticating said originating access device using a second PHY channel; and

hosting said communication session over a third PHY channel, said third PHY channel established between said access point and said originating access device.

16. The machine-readable storage according to claim 15, comprising code for generating at least one encryption/decryption key for use during said communication session.

17. The machine-readable storage according to claim 16, wherein authenticating code comprises code for requesting authentication information from an authentication server.

18. The machine-readable storage according to claim 17, comprising code for delivering at least a portion of said authentication information received from said authentication server to said originating access device via said second PHY channel.

19. The machine-readable storage according to claim 18, comprising code for delivering said at least one encryption/decryption key to said originating access device via one of said first PHY channel or said second PHY channel.

20. The machine-readable storage according to claim 15, comprising code for receiving an identification of said originating access device by said access point.

21. The machine-readable storage according to claim 20, wherein said identity of said originating access device is one or more of a WEP key, a MAC address, and/or an IP address.

22. The machine-readable storage according to claim 15, comprising code for acknowledging said received request on said first PHY channel.

23. The machine-readable storage according to claim 15, comprising code for determining a type of traffic generated by said originating access device on said first PHY channel.

24. The machine-readable storage according to claim 23, comprising code for generating at least one encryption/decryption key dependent on said determined traffic type.

25. The machine-readable storage according to claim 24, comprising code for distributing said generated at least one encryption/decryption key via one or both_of said second PHY channel and/or said third PHY channel.

26. The machine-readable storage according to claim 15, comprising code for establishing at least one virtual channel between said originating access device and a terminating access device.

27. The machine-readable storage according to claim 26, comprises code for tunneling information between said originating access device and said terminating access device.

28. The machine-readable storage according to claim 26, comprising code for establishing at least a portion of said at least one virtual channel over at least a portion of one of said first PHY channel, said second PHY channel or said third PHY channel.

29. A system for multiple encryption in a multi-band multi-protocol hybrid wired/wireless network, the system comprising:

at least one receiver of an access point adapted to receive on a first PHY channel, a request for initiation of a communication session from an originating access device;

at least one authenticator adapted to authenticate said communication session by authenticating said originating access device using a second PHY channel; and

a third PHY channel being adapted to facilitate hosting of said communication session, said third PHY channel established between said access point and said originating access device.

30. The system according to claim 29, wherein said at least one authenticator is adapted to generate at least one encryption/decryption key for use during said communication session.

31. The system according to claim 30, wherein said at least one authenticator is adapted to receive requests for authentication information.

32. The system according to claim 31, wherein said authenticator is adapted to deliver at least a portion of said authentication information received from said authentication server to said originating access device via said second PHY channel.

33. The system according to claim 32, wherein said at least one authenticator is adapted to deliver said at least one encryption/decryption key to said originating access device via one of said first PHY channel or said second PHY channel.

34. The system according to claim 29, wherein said at least one receiver is adapted to receive an identification of said originating access device by said access point.

35. The system according to claim 34, wherein said identity of said originating access device is one or more of a WEP key, a MAC address, and/or an IP address.

36. The system according to claim 29, wherein said at least one receiver is adapted to acknowledge said received request on said first PHY channel.

37. The system according to claim 29, wherein said at least one authenticator is adapted to determine a type of traffic generated by said originating access device on said first PHY channel.

38. The system according to claim 37, wherein said at least one authenticator is adapted to generate at least one encryption/decryption key dependent on said determined traffic type.

39. The system according to claim 38, wherein said at least one authenticator is adapted to distribute said generated at least one encryption/decryption key via one or both of said second PHY channel and/or said third PHY channel.

40. The system according to claim 29, wherein said at least one receiver is adapted to establish at least one virtual channel between said originating access device and a terminating access device.

41. The system according to claim 40, wherein said at least one receiver is adapted to tunnel information between said originating access device and said terminating access device.

42. The system according to claim 40, wherein said at least one receiver is adapted to establish at least a portion of said at least one virtual channel over at least a portion of one of said first PHY channel, said second PHY channel or said third PHY channel.

EVIDENCE APPENDIX
(37 C.F.R. § 41.37(c)(1)(ix))

(1) USPP 20030140131 ("Chandrashekhar"), entered into record by the Examiner in the May 7, 2009 Final Office Action.

(2) USP 6,751,729 ("Giniger"), entered into record by the Examiner in the May 7, 2009 Final Office Action.

(3) USP 7,174564 ("Weatherspoon"), entered into record by the Examiner in the May 7, 2009 Final Office Action.

(4) USP 6,088,451 ("He"), entered into record by the Examiner in the May 7, 2009 Final Office Action.

RELATED PROCEEDINGS APPENDIX

(37 C.F.R. § 41.37(c)(1)(x))

The Appellant is unaware of any related appeals or interferences.